VZCZCXYZ0004
RR RUEHWEB

DE RUEHSP #1099/01 3051743
ZNR UUUUU ZZH
R 011743Z NOV 07
FM AMEMBASSY PORT OF SPAIN
TO RUEHC/SECSTATE WASHDC 8766
INFO RUEAHLC/HOMELAND SECURITY CENTER WASHDC
RUEAIIA/CIA WASHDC
RHEHNSC/NSC WASHDC

UNCLAS PORT OF SPAIN 001099

SIPDIS

SENSITIVE
SIPDIS

DEPT FOR S/CT--MCCUNE;CIA FOR NCTC

E.O. 12958: N/A
TAGS: ASEC CVIS KVPR PGOV PINR PREL PTER TD KHLS
SUBJECT: PRACTICES OF THE GOVERNMENT OF TRINIDAD AND TOBAGO ON INFORMATION COLLECTION, SCREENING, AND SHARING

REF: (A) STATE 133921 (B) 06 STATE 190832 (C) 06 PORT OF SPAIN 01035

SENSITIVE BUT UNCLASSIFIED, PLEASE PROTECT ACCORDINGLY

¶1. (SBU) This cable responds to questions in ref A. Questions in ref B were previously answered in ref C.

Watch listing

¶2. (SBU) The Government of Trinidad and Tobago (GOTT) maintains both an &alert list8 of individuals who should be immediately detained upon entry and a &watch list8 of people whose entry into T and T is made known to appropriate agencies for monitoring of movements, etc. The number of names on this list is unknown, although interlocutors have indicated that there are &too many8 names and that the lists should be culled. The watch list and alert list are maintained by the Ministry of National Security.

Traveler Information Collection

¶3. (SBU) The GOTT collects information from travelers arriving in Trinidad and Tobago based on regulations in the Immigration Act. The travel documents of passengers arriving by air and sea, including passengers and crew of yachts and similar craft, are examined in the same manner by immigration officials. Although policies are the same for arrivals by air and sea, a slight difference in regulations calls for more intensive monitoring of maritime arrivals, although this is not always practiced; one difficulty is that immigration officials monitoring maritime arrivals are generally presented with a paper list of names of passengers and crew and their nationality and passport information, making rapid screening difficult. The GOTT may share information on individual travelers with foreign governments on a case by case basis if requested; there is no formal policy authorizing this, and information is not shared on a routine basis. During the Cricket World Cup in 2007, various Caribbean nations cooperated on sharing data, but this practice lapsed in T and T due to a sunset clause. The GOTT collects passenger name record (PNR) data on incoming commercial flights or vessels, but this is sometimes in hard copy on paper. U.S. Customs is currently working with T and T Customs and Excise officials to automate passenger lists and enter and retrieve them electronically. PNR data is currently available to systematically screen travelers for intelligence or law enforcement purposes, but in practice arrivals by sea are more difficult to screen. The GOTT does

not have any existing treaties to share PNR data. Although the electronic travel authority systems and the data base currently in place have been used to detect security threats, including wanted criminals, an interlocutor has commented that sometimes too many names are flagged without sufficient accompanying data on reasons to detain or monitor an individual.

Border Control and Screening

¶4. (SBU) The GOTT employs new software that has certain algorithms to screen travelers of security interest, but it is not certain that this has been activated for daily use. All travelers, both T and T citizens and other nationals, are recorded and tracked. There is no data available on the frequency with which travelers are admitted with ostensibly bona fide documents that are not electronically recorded. Unrecorded entries and exits by persons arriving by boat from Venezuela at locations other than official ports of entry are frequent; the number of such entries and exits may be between five and ten percent of all entries and exits. There is legislation in place authorizing border control officials to use other criminal data when deciding who can enter the country. Individuals attempting to enter without valid travel documents are referred by officials of the Immigration Division of the Ministry of National Security to the Special Branch Police, who detain them until they can be sent back to the country from which they arrived. Individuals are sometimes sent back without being questioned on the provenance of their false documents, although recently more of them have been questioned regarding their reasons for attempting to enter T and T illegally before they are sent back to their previous point of origin. Government policies on questioning, detaining and denying entry to individuals

presenting themselves at a point of entry follow regulations in the Immigration Act; the GOTT also refers to International Conventions to which it is a signatory. Information sharing within and among agencies of the GOTT has traditionally been sporadic, irregular, and not adequate for making rapid decisions or taking quick action. Recently, due to personal contacts among agencies formed by training together, this situation has begun to improve slightly.

Biometric Collection

¶5. (SBU) The only biometric in the GOTT border control system installed by the Canadian Banknote Company is facial recognition capability. Officials of the Immigration Division are not legally authorized to take or collect fingerprints. There is some discussion of using fingerprint biometrics in the passport application process.

Passports

¶6. (SBU) The GOTT began to issue machine readable passports in June of 2007; these passports include facial recognition features. The GOTT does not share the public key to read data with other governments. However, the system in place can read biometric data from other countries, provided they have made the key available. The GOTT issues a standard passport with the normal five-year validity to replace a passport that has been lost or stolen. There are no standard procedures in place for bearers who frequently report their passports lost or stolen. However, each application to replace a stolen passport must be accompanied by a police report. The older style passport that was easier to alter was more likely to be reported lost or stolen than the newer machine readable passport. In most cases, a new standard passport with no distinctive identifying features is issued with a full five years, validity. Post has not noticed an increase in the number of passports with no record of prior travel being used to apply for U.S. visas. There is an emergency passport that has a white cover (the regular

passport is dark blue) and has its own series of serial numbers.

Fraud Detection

¶7. (SBU) There is a fraud unit within the police that investigates various instances of fraud, including the use of fraudulent documents. In addition, as part of a training program conducted by the IOM, immigration officials are being issued hand-held scanners, loupes, and combination loupes and infrared and black light devices with which to examine passports. The GOTT will also reportedly subscribe to the Edison database, which provides examples of all passports in the world and their identifying features.

Privacy and Data Security

¶8. (SBU) The immigration and data base system currently in use reportedly contains information on previous deportations. Records related to questioning, detention or removal of individuals are kept on file indefinitely, usually in locked filing cabinets. The collection and use of sensitive data is restricted by privacy laws; however, data is shared among GOTT entities as required. Post is not aware of any requirement to provide notice to the public concerning the implementation of new databases of records; post is also unaware of laws relating to security features for government computer systems that hold personally identifying information. The Freedom of Information Act would allow an individual to request access to data, either raw data or case file data that domestic security agencies hold about him; however, there are some prescribed exceptions to the type of data that must be made available. A non-citizen does not have the right to sue the GOTT to obtain data held by a government security agency about him.
KUSNITZ